State of Connecticut

Network Domain
Technical Architecture

January 4, 2001

Version 1.0

History of Changes

12/05/2000	In LAN Standards Totally revised Standard 3, LAN Protocols to be TCP/IP with new rationales In WAN Standards Standard 1 TCP/IP is now the WAN standard; also added new rationale. In Wireless Standards Added CDPD to Standard 1
11/29/00	Added Appendix – Network Security Policy and Procedures for use by all State Agencies

Table of Contents

History of Changes 2
Table of Contents 3
Mission Statement 6
Introduction and Background 6
Principles 9
Principle 1: The Network provides an infrastructure to support all communications and application requirements 9
Principle 2: The Network is available 24x7x365. Access to the network can be anytime from anywhere. 9
Principle 3: Networks must be designed for growth, flexibility and quick adaptability. 9
Principle 4: Networks must be designed with safety and security of data being a high priority. 9
Principle 5: The network must use industry-proven, mainstream technologies, with priority given to network products adhering to industry standards, open architecture, and de-facto standards 9
Principle 6: The network must be manageable and be maintained in a way that provides proactive response capability, Service level agreement statistics and a total cost of ownership model that is beneficial to the State. 10
Component Architecture 11
A) Local Area Network (LAN) 11
1) Technology Components 11
2) Standards 14
Obsolete 15
Transitional 15
Strategic 15
Research / Emerging 15
Standard 1: The standard for LAN cabling is Category 5E UTP. 16
Standard 2: Link layer access protocol, Ethernet IEEE 802.3, is the standard. 16
Standard 3: The standard LAN protocol is TCP/IP. 16
Prospective Standard 4: IEEE 802.11b Wireless LAN. 16
Standard 5: Switching is the standard for LAN device connectivity. 16
3) Recommended Best Practices 17
Best Practice 1: Networks must be positioned for future growth in traffic, expansion of services, voice, data, video, imaging and wireless. 17
4) Implementation Guidelines 17
Guideline 1: Configure the topology (physical wiring) in a Star pattern. 17
Guideline 2: Use switched multi-segment design with managed hubs and switches. 18
Guideline 3: Cabling should follow TIA/EIA standards for media, spaces and pathways, administration and testing. 18
B) Wide Area Network (WAN) Architecture 18
1) Technology Components 19
Technology Component 1: Protocols 19
Technology Component 2: Customer Premise Equipment (CPE) 19
Technology Component 3: Carrier Services 20

Technology Component 4: Internet Access 21
2) Standards 22
Standard 1: The WAN standard protocol is TCP/IP. 22
Standard 2: The standard internet access technology is Domain Name System (DNS) and IP address assignments are provided by Department of Information Technology (DOIT) for those agencies participating in the DOIT Enterprise Network Infrastructure. 22
Standard 3: When connecting to the State Infrastructure via the Internet, encryption must be used. 23
Standard 4: Dialup remote access must use authentication and in some insistences encryption 23
3) Recommended Best Practices 23
Best Practice 1: Develop an enterprise-wide network infrastructure that is scalable, centrally managed with quality of service (QOS), class of service (COS) and policy base. 23
Best Practice 2: When industry standards do not exist, use de-facto product standards .. 23
Best Practice 3: Configure WAN protocols using TCP/IP. 24
Best Practice 4: DOIT supports EIGRP on the routers in the infrastructure. 24
4) Guidelines 24
Guideline 1: Must contact Department of Information Technology (DOIT) for connection to the State Infrastructure. 24
C) WIRELESS : TDMA, CDMA, CDPD, GSM 24
1) Standards 25
Standard 1: TDMA, CDMA, CDPD and GSM for cellular telephone communications.. 25
2) Recommended Best Practices 25
Best Practice 1: Still being developed 25
3) Guidelines 25
Guideline 1: Still being developed 25
D) Video and Imaging 25
1) Standards 26
Standard 1: H.320 interoperability standards. 26
Prospective Standards 2: ITU H.323 interoperability standards, IETF Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), Motion Pictures Experts Group standards (MPEG). 26
2) Recommended Best Practices 27
Best Practice 1: Still being developed 27
3) Guidelines 27
Guideline 1: Still being developed 27
E) PBX 27
Technology Component: Private Branch Exchange (PBX) 27
1) Standards 27
Standard 1: ISDN PRI compatibility. 27
Standard 2: Analog services compatibility. 28
Standard 3: T-1 compatibility. 28
2) Recommended Best Practices 28
Best Practice 1: Still being developed 28
3) Guidelines 28

Guideline 1: Still being developed..... 28
Product Selection 29
Appendix – Network Security Policy and Procedures for use by all State Agencies 30
Purpose 30
Policy Statements..... 30
Implementation of the Policy 31
Agency Planning and Reporting Responsibilities 31
Planning: 31
Reporting:..... 31
Compliance: 32
Scope..... 32
Definitions 32

Mission Statement

Connecticut's network architecture delineates a reliable, resilient infrastructure that supports the state's communications and application requirements in an efficient manner. The Department of Information Technology (DOIT) designs, implements and manages the State infrastructure and backbone.

Introduction and Background

In defining the state's communications infrastructure, the network architecture sets forth a formal means of documenting the appropriate approach to be taken to ensure that the network is up to the task of fully supporting the services for which it is required.

To provide this definition, a number of factors are taken into account. These are based on decision criteria that are, without the structure and guidance of architecture, sometimes incorporated on a piecemeal basis into various business decisions that affect the ongoing use and growth of the network. These decisions can often occur as part of procurement activities and deployment of individual applications, without regard to the entire enterprise. Among other factors, these criteria might include:

- Costs, both initial and ongoing
- Bandwidth requirements
- Reliability
- Network management
- Maintenance and support
- Standards
- Scalability
- Strategic support of business direction
- Strength of product and service providers
- Technology viability
- Universal accessibility
- Multimedia support
- Security

Although these and other criteria are necessary considerations, they can too often be harmful to the long-term strategies of an organization if they are used in an incomplete manner, or if they are used in isolation without consideration to all factors in appropriate measure. For example, cost control could be sacrificed in order to obtain a high level of security (as in encryption for all transactions), and conversely security could suffer if too much emphasis is placed on controlling costs. Neither scenario is acceptable, yet the intermittent or partial use of these criteria as part of isolated business decisions can have this detrimental effect.

The formal development of the network architecture serves to bring together all relevant criteria so that a balance can be struck. Naturally, the process of developing the architecture causes a great number of decisions to be made. It is these decisions that essentially comprise the architecture. Will we encrypt all transactions? Probably not! Will we support encryption of certain critical transactions? Absolutely! The formal architecture development process allows these countless issues to be addressed as considerations on a broad scale, rather than as part of deployment of an individual application. The decisions made as part of the architecture

development process will limit or eliminate certain options for future network components or services. This is likely to cause concern among parties who may already utilize certain products for their in-place networks. These parties must be allowed to participate in the architecture development process so that their current investment in these products can be maximized while also developing a transition plan to allow certain obsolete or non-conforming products to be phased out. Maximizing the investment and transitioning, these products should not be seen as mutually exclusive activities, as both are in the best interests of the enterprise. Developing the timing, funding, and resource plan to accomplish this balancing act is time consuming, but key to successful transitioning toward the target architecture.

The development of the network architecture is a continuous process, and this is especially important in an environment where: 1) Funds to instantly deploy the desired infrastructure are not available; and 2) Many of the criteria relating to business requirements, technology, and product providers are changing constantly. This continuous process provides an opportunity to continually refine the architecture to keep it aligned with business strategies, and the amount of effort required creates an opportunity to eventually engage all parties who might have an interest in the use of the network infrastructure.

Involving these parties allows the architecture to 1) Adequately reflect the true needs of the organization; 2) Ensure that products are adequately reviewed due to the diversity of knowledge that is inherently incorporated into the process; and 3) Provide a means of communication and understanding of the architecture among the key people involved in the utilization, design, management, and maintenance of the network resources. Each of the parties involved in the process become an essential part of maintaining the architecture since they are then well positioned to explain the Rationale behind the architecture to others. These people can bring feedback to future iterations of the architecture development process as part of their encounters with others, and they can prevent misunderstanding that might otherwise result with network users who are not aware of the decision criteria that comprised the architecture development process. This is especially critical in order to prevent exceptions to the architecture on a case-by-case basis, and to preserve the integrity of the network.

Especially in the development of a network architecture, it is important to keep in mind that there may be many decisions that are not “right” or “wrong.” The value of the decision process is not necessarily the specific outcome, but the fact that a decision has been made and will be adhered to. The numerous small decisions, many with interdependencies, are the architecture when taken in their entirety. The network architecture, developed in this way, serves to facilitate the numerous business processes that are used in deploying the network since critical choices have already been made. Budgeting becomes predictable. Specifications are uniform and can be reused. Secure transactions are truly secure across the network. Building wiring does not require a new topology with each project. Network devices comply with management standards in a uniform manner. Disaster recovery and alternate network facilities are designed into each network project. As the network architecture develops and is implemented over a period of time, these benefits manifest themselves in terms of faster implementation of network services, lower support costs, and a reliable, resilient infrastructure that supports the state’s communications and application requirements in an efficient manner.

The following types of networks are discussed in this chapter:

Local Area Networks (LAN). A communications network that serves users within a confined building or geographical area. It can be made up of hub/switches, wiring, servers, workstations,

printers, network operating system and a communications link. Servers are high-speed machines that hold programs and data shared by network users. The workstations (clients) are the users' personal computers, which perform stand-alone processing and access the network servers as required. The controlling software in a LAN is the network operating system (NetWare, UNIX, Windows NT, etc.) that resides in the server. A component part of the software resides in each client and allows the application to read and write data from the server as if it were on the local machine.

Diskless and floppy-only workstations are sometimes used, which retrieve all software and data from the server. Increasingly, "thin client" network computers (NCs) and Windows terminals are also used. A printer can be attached locally to a workstation or to a server and be shared by network users. A LAN can operate between 10 Mbps and 2 Gbps(billion bits per second).

Wide Area Network (WAN). A communications network that covers a wide geographic area, such as state or country. The WAN is implemented using private or public carrier provided lines. A WAN typically serves as a customized communication "link" that interconnects all of an organization's local networks with communications trunks designed for the anticipated communication speed between the LAN's. The existence of a WAN permits the deployment of central or remote managed file, print, or application servers across the infrastructure..

Internet. A global network of limitless interconnected LANs, enabling computers of all kinds to directly and transparently communicate and share services throughout the world. The Internet also constitutes a shared global resource of information, knowledge, and means of collaboration, and cooperation among countless diverse communities.

Intranet. A private network for intra-business communications using Internet software and standards. Its popularity is growing fast because of its usefulness in collaborative work styles across workgroups, campuses, and even geographical barriers with a high degree of "behind the firewall" security. The difference between an Internet and an Intranet is that an Intranet provides connectivity between specific sites in a pre-determined infrastructure for business units, customers, or designated participants. An Intranet is often protected from outside access by a firewall. A firewall is a hardware/software device that can block traffic between networks or specific host computers.

WANs support the cooperative and collaborative functions within the corporation or enterprise. Business requirements necessitate using a variety of applications on the networks. The use of uniform network architecture will enable LANs within the WAN to inter-operate while allowing a broad platform on which to run applications as needed. Such interoperability requires cooperation at all State levels and consistency in network components (e.g. wiring, hubs, servers, operating systems, and protocols), management practices, and services.

Note: Additional information about Wireless Networking, Inter/Intranet, Voice Services, and Video Network Services will be added to this Network Chapter in future releases.

Principles

Domain principles are intended to guide the evaluation selection, design, construction and implementation of the domain and elements.

Principle 1: The Network provides an infrastructure to support all communications and application requirements

Rationale:

The network today is a global highway. It must be positioned to enable access to information regardless of the method of delivery, or the location of the client. The network is the essential enabling technology for a variety of information, resources and applications. In addition to supporting the immediate scope, the infrastructure must be positioned to support transparently, public business entities that are required to perform State services.

Principle 2: The Network is available 24x7x365. Access to the network can be anytime from anywhere.

Rationale:

Networks have become a critical and integral part of the Federal, State, and local business functions and processes. Failure of any single element can have a severe and adverse effect on one or more business applications or services. Reliable networks contain no single point of failure. Fault tolerance and reliability must be built-in. Network access and usage must minimize latency. Data must pass across the network in a timely manner so that business decisions can be based on up-to-date information. Network must support both E-Commence and M-Commence

Principle 3: Networks must be designed for growth, flexibility and quick adaptability

Rationale:

IP protocol must be used by all network solutions. This will provide the scalability, flexibility, and consistency to respond to changing business requirements. Open protocols give the State the opportunity to take advantage of scalable/modular off the shelf components thereby reducing the time to respond to business requirements. The use of TCP/IP enlivens the State to support common access to public networks and applications while minimizing the total cost of ownership

Principle 4: Networks must be designed with safety and security of data being a high priority.

Rationale:

State business operations and applications are valuable State assets. Therefore, Enterprise network systems will be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes. Clients who need to access the Infrastructure from private or public networks must obtain authorization and authentication under the guidelines set by the enterprise. Attention must be paid to new and emerging technology, such as Biometrics technology and wireless.

Principle 5: The network must use industry-proven, mainstream technologies, with priority given to network products adhering to industry standards, open architecture, and de-facto standards

Rationale:

Adhering to Industry Standards will help avoid the dependence on weak vendors and yet give us the flexibility of using de-facto standards where there is a clear technology advantage in utilizing a vendor who is a leader in developing technological network infrastructure. This will ensure robust product support and enable greater use of commercial off the shelf solutions.

Principle 6: The network must be manageable and be maintained in a way that provides proactive response capability, Service level agreement statistics and a total cost of ownership model that is beneficial to the State.

Rationale:

Customers require a certain level of service. A centrally developed and managed infrastructure provides a more cost-effective use of infrastructure resources and allows for leveraging skills across the enterprise to deliver this service. Reliable networks contain no single point of failure. Networks are comprised of many components, and are only as reliable as the weakest link. Reliability and scalability must be built-in, not added-on. To insure delivery of these services, class of service and content policy management functionality will be applied.

Component Architecture

A) Local Area Network (LAN)

Overview

The invention of the microcomputer brought computer-processing power to the individual desktop. Users were able to have hands-on control of the accumulation, manipulation, and display of their own information. As such functionality became commonplace in the work area, users began to recognize the need to share information and resources with other users in their immediate area. Thus, local area networks (LANs) were developed to connect Statewide Technical Architecture Document devices, such as standalone workstations and printers, in a limited geographic area such as a single building, a cluster of buildings, or a campus type arrangement.

The initial LANs simply offered a means for users to share system resources, such as information and input or output devices. A network operating system (NOS) was used to accomplish this set of functions for the LANs. Over time, users began to require more functionality from these simple networks. Users wanted to expand the functions that could be performed on a LAN. Users also wanted to communicate with users and sites outside of their own work area. Thus, LANs were enhanced to offer support for a multitude of business applications. Application servers were added to the LANs in order to provide a multi-faceted, flexible environment. In addition, technology was augmented to allow communication between LANs through wide area networking techniques.

1) Technology Components

The following technical components are necessary for the successful implementations of LANs:

(1) Topology

The way a network is physically wired refers to the network topology. There are three topologies used today, bus, ring, and star (see figure 1 below).

In a bus topology, each device is connected to the network in a sequential manner so that, if the connection of one device on the LAN fails, the whole network fails. A ring topology connects devices in a closed loop. As with the bus topology, a problem with a single connection in a ring network will cause a failure from that point on the ring to the end. The star topology uses a central hub or switch to which each network device is connected. Problems with a connection in a star network only affect that one device. Because each network device is attached individually, a star topology provides the capability to easily add and remove devices as necessary. Today’s computing environments are dynamic infrastructures in which network configurations are constantly tuned, upgraded, and modified in order to meet changing demands and technology innovations. The star topology responds well to such demands.

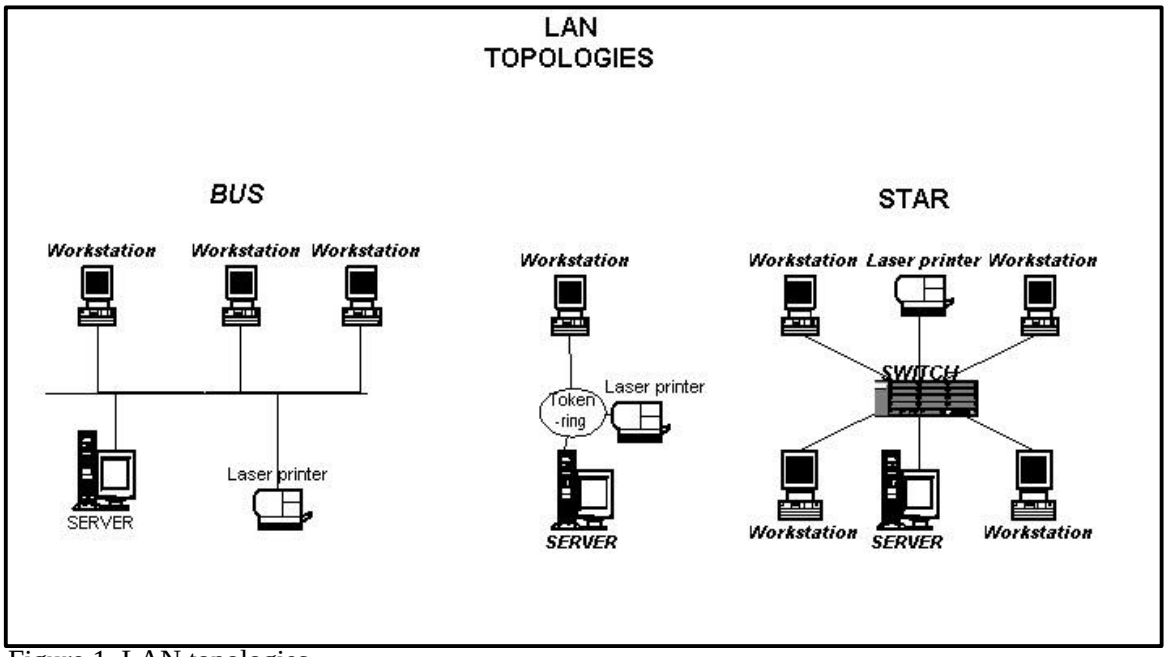

Figure 1. LAN topologies

(2) Protocol

For two devices to communicate within a network they must both speak the same language or protocol. When devices do not use the same network protocol, they must use an interpretive device, or gateway, that translates the language one device uses into a language another device can understand. Coordinating the use of protocols across an enterprise WAN enables the State to minimize the necessity for translations and, thereby, reduce support and capacity requirements.

The Institute of Electrical and Electronics Engineers (IEEE) is the organization primarily responsible for establishing standards for network protocols. The most widely used standards are IEEE 802.5 (Token Ring) and IEEE 802.3 (Ethernet). IEEE can support 10/100 Mbps. Emerging high performance protocol include 802.3ab Gigabit Ethernet. Gigabit will support multi-media communication technology that can handle telephony and video as well as conventional data.

Asynchronous Transfer Mode (ATM) at one point in time was thought to be a viable LAN technology but not any longer. The most widely accepted forms of Ethernet are 10BaseT Ethernet and 100BaseT Fast Ethernet. The number in the name stands for the signal speed in megabits per second (Mbps). The Base means that devices on the network transmit using the network's entire bandwidth (e.g., 10 Mbps or 100 Mbps). The T stands for twisted pair wiring. Used in a star topology, 10BaseT and 100BaseT are a reliable, scaleable, and maintainable choice. 100BaseT Fast and 1000Base T Ethernet has the bandwidth necessary to support the needs of future voice and video requirements.

(3) Cabling

The basic component of each network topology is the cabling. Cabling options for the network depend upon the particular requirements of a LAN. Factors such as the distance between devices, volume of throughput, number of devices and network topology can determine what type of cabling is best suited for the LAN. When looking at the cabling of a network, the rule of thumb is that the technology used should have an expected useful life of approximately 8 years. The types of network cabling most commonly used are:

- *Twisted pair.* Twisted pair cabling comes in both shielded (STP) and unshielded (UTP) types. STP cable is primarily used in Token-Ring environments. UTP supports almost all network applications such as voice, Token-Ring, Ethernet, and even Asynchronous Transfer Mode (ATM). A chosen Category 5E UTP should be certified for 100 MBPS. Newer grades of UTP are being developed to support higher speed technologies such as gigabit Ethernet.
- *Coaxial cable.* Coaxial cabling is generally used for video application.
- *Fiber optic.* Uses light impulses instead of electrical impulses to transmit data from point A to point B. It can carry a signal further than copper cabling and can meet demands for higher bandwidth. It is often used in conjunction with other cabling, for vertical MDF, in buildings to provide a network backbone between hubs and switches.

(4) Hubs and Switches

In an Ethernet network, each device is cabled to the LAN hub in a star topology. This hub contains one port for each device connected to it. Hubs act as the LAN “traffic cop” allowing streams of information traffic to flow between the ports in an orderly manner. In the event a port is busy the hub provides a buffer to hold the information until the port is freed up. The hub is an ideal point for network management due to its central location and because all network traffic flows through it. The hub is not favorable to security, since all the traffic flows between the ports (see Figure 2 below)

Network Switches are multi-port bridges, but share some characteristics as routers. Like routers, switches divide the network into a number of network segments (each physical switch port can be considered as a separate network). Each port can operate without interference from traffic local to any other segment. Switching is performed at layer two of the seven-layer model, the same as bridging. Switches can be used in conjunction with or instead of hubs. Through the use of switching, network traffic is balanced across multiple segments thus reducing resource contention and increasing throughput capacity. Switches are also used to improve security thorough port segmentation.

Switches enable network managers to divide networks into Virtual LANs (VLANs). A VLAN is basically a limited broadcast domain, meaning that all members of a VLAN receive every broadcast packet sent by members of the same VLAN but not packets sent by members of a different VLAN. All the members of a VLAN are grouped logically into the same broadcast domain independent of their physical location. Adds, moves and changes (MACs) are achieved via software within a VLAN. No routing is required among members of a VLAN.

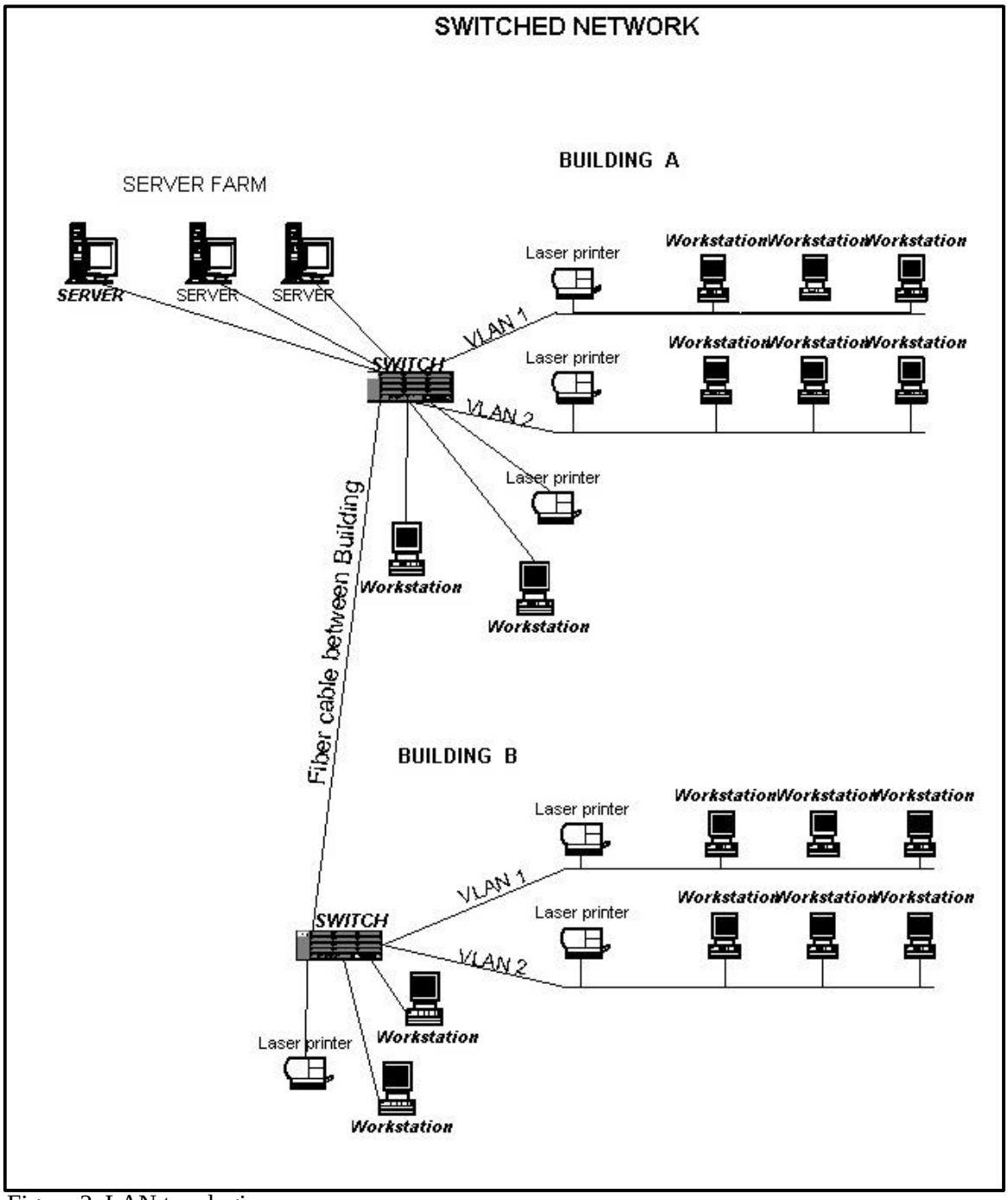

Figure 2. LAN topologies

2) Standards

Standards in the Statewide Technical Architecture document are a specific implementation of a technology and are mandatory, as opposed to desirable.

The following standards have been established to assist agencies in the implementation of LANs. The goal is to employ only open systems based on industry approved standards, but a full complement of open standards does not yet exist for all components of LANs. Therefore, a combination of industry standards, de facto industry standards, mutually agreed upon product standards, and open standards are currently required to support the state's heterogeneous

operating environment. All standards will be periodically reviewed, when available and feasible, and new standards and resources will be identified.

The following categories were used to describe each technical standard and product standard.

Obsolete

It is highly likely that these standards or products, while still in use, will not be supported by the vendor (industry, manufacturer, etc.) in the future. Some products and standards have already reached the non-supported state. Plans should be developed by the agencies or the State to rapidly phase out and replace them with strategic standards or products. No development should be undertaken using these standards or products by either the agencies or the State.

Transitional

These are standards or products in which an agency or the State has a substantial investment or deployment. These standards and products are currently supported by DOIT, the agencies, or the vendor (industry, manufacturer, etc.). However, agencies should undertake development using these standards or products only if there are no suitable alternatives that are categorized as strategic. Plans should be developed by the agencies or the State to move from transitional to strategic standards or products as soon as practical. In addition, the State should not use these standards or products for development.

Note: many older versions of *strategic* standards or products fall into this category, even if not specifically listed in a domain architecture document.

Strategic

These are the standards and products selected by the state for development or acquisition, and for replacement of *obsolete* or *transitional* standards or products. (Strategic means a three to four year planning horizon.) When more than one similar strategic standard or product is specified for a technology category, there may be a preference for use in statewide or multi-agency development. These preferred standards and products are indicated where appropriate.

Note: some strategic products may be in “pilot testing” evaluation to determine implementation issues and guidelines. Pilot testing must be successfully completed prior to full deployment by the agencies or the State.

Research / Emerging

This category represents proposed strategic standards and products that are in advanced stages of development and that should be evaluated by the State. The some of these standards or products may already be undergoing “hands-on” evaluation. Others will need to be tracked and evaluated over the next 6 to 18 months.

Standard 1: The standard for LAN cabling is Category 5E UTP.

Rationale

- Anticipate adoption of Cat 6 standard by mid 2001 by the TIA /Electronic association.
- Cat 7 is still in development. TIA 568 standard includes fiber and copper.
- Unless specific needs exist, such as high EMI or long distances, UTP should be utilized for the horizontal runs in cable layouts and fiber for the vertical risers.
- CAT 5E UTP can be certified to carry 10/100/1000 MBPS of data.
- It is an industry standard wiring plan and has the support of the IEEE.
- Wiring, cable, connector, and equipment vendors have standardized on this cabling.

Standard 2: Link layer access protocol, Ethernet IEEE 802.3, is the standard.

Rationale

- Widely accepted format.
- Reliable, the protocol has been used for years and is very stable.
- Scaleable, faster versions are currently emerging to help manage the increase of data flow.
- 1000BaseT Gigabit Ethernet has the bandwidth necessary to support the future technology, voice, video and imaging.

Standard 3: The standard LAN protocol is TCP/IP.

Rationale

- Open protocol.
- Allows Internet access.
- Allows for seamless integration of Intranet, Extranets and VPNs
- Supported by all vendors.

Prospective Standard 4: IEEE 802.11b Wireless LAN.

Rationale

This standard offers a relatively high speed (11Mb/s) wireless connection and the wireless LAN manufacturers have adopted this as a result of its adoption as an IEEE standard. The state will need to perform testing and deployment of systems prior to adopting this standard.

Standard 5: Switching is the standard for LAN device connectivity.

Small field offices and work groups, with limited needs, a hub will be acceptable. Before using a hub, you must consider manageability, applications and performance. Security is limited.

Rationale

- Provides scalability and better throughput
- Network switches provide the ability to break a network up into smaller sub-network segments.
- Switches enhanced security,
- They improve LAN performance. With switching, network traffic is balanced across multiple segments thus reducing resource contention and increasing throughput capacity.

- Switching allows networks to assign increased speed or performance capability to particular segments in order to respond to heavy usage or application requirements using QoS or Ethernet channel.
- All network hub and switches must be SNMP managed.

3) Recommended Best Practices

Recommended Best Practices in the Statewide Technical Architecture document assist agency staff in the planning, design, implementation and expansion, administration, maintenance, and support of LANs. They are based on experience and proven results. They employ standards and practices designed to support a uniform LAN.

Best Practice 1: Networks must be positioned for future growth in traffic, expansion of services, voice, data, video, imaging and wireless.

Rationale

The increasing investment of funds in network infrastructures dictates that the life span of each additional component or enhancement be as long as possible. This can be accomplished if the design supports current needs but includes an anticipated growth potential. For example, installing Category 5E cabling today to run a 10mbps network positions a site to upgrade to a 100mbps speed in the future without replacing the cabling.

As businesses expand, networks expand. A flexible, open network design will allow a business to minimize the costs and disruptions of configuration management while providing timely and responsive network changes when and where required.

4) Implementation Guidelines

Table 1. Implementation Approach for LANs

Transitional	**Strategic Technology**	**Research / Emerging**
Bus or Ring topology	Star topology	
Token Ring protocol	10BaseT Ethernet, 100Base T Ethernet	Gigabit switching,
Coaxial cabling Category 3,5 UTP	Category 5 UTP Category 5E UTP	Category 6, Category 7, or Fiber optics
Single segment design with unmanaged hubs	Switched, multi-segment design with managed hub or switch	Dynamic switching to the Desktop, ATM Gigabit
IPX protocol	TCP/IP	Gigabit switching,

The implementation guidelines in this section pertain to LANs.

Guideline 1: Configure the topology (physical wiring) in a Star pattern.

Rationale

- Star topology uses a central hub/switch to which each network device is connected.

- Problems with a connection in a star network only affect that one device.
- A star topology provides the capability to easily add and remove devices as necessary.
- A star topology responds well to dynamic infrastructure changes in order to meet the growing demands of data movement. With ever increasing demands of information movement, more data, secure paths, new paths, and faster access, a star topology allows different, changeable, connections.

Guideline 2: Use switched multi-segment design with managed hubs and switches.

Rationale

- Hubs should only be used in small environments, 12 nodes or less.
- The hub is an ideal point for network management due to its central location and because all network traffic flows through it.
- Network switches provide the ability to break a network up into smaller sub-network segments.
- Hub and switch must be SNMP manageable
- Switches enhanced security,
- Switches can be used in conjunction with hubs.
- When stacking switches. The type of application and amount of traffic must be taken into consideration for performance reasons. Standard practice, switches should not be stacked any more than three deep.
- Uplinks on switches should be configured at the highest bandwidth.
- Performance between switches can be affected when attaching a hub to a switch.
- Never attach a switch to a hub.
- They improve LAN performance. With switching, network traffic is balanced across multiple segments thus reducing resource contention and increasing throughput capacity.
- Switching allows networks to assign increased speed or performance capability to particular segments in order to respond to heavy usage or application requirements using QoS or Ethernet channel.

Guideline 3: Cabling should follow TIA/EIA standards for media, spaces and pathways, administration and testing.

- Testing should ensure full documented certification of media (CAT 5E and fiber) performance.
- Documentation certification should be in the form of paper and CD.

B) Wide Area Network (WAN) Architecture

Overview

Before computers, the only way to exchanges information from remote sites was via the telephone. The language (protocol) was always in synchronization with the receiver. When mainframes were introduced, a method was needed to connect from remote sites. Initially, the remote devices were non-intelligent and had to connect using a multiplexor or control unit. This was the beginning of the WAN. A WAN connects local sites together through the use of a private or public communication line. The WAN can be thought of as an integrated vehicle, which is customized (speed) to interconnect all of the State's local networks. The existence of a WAN permits the deployment of central or remote managed file, print, or application servers

across the infrastructure. Policies, quality of service in addition to class of service can be applied to enhance the performance, scalability and flexibility of the enterprise. From policies, we can then derive service level agreements (SLA) to ensure enterprise delivery performance from WAN vendors.

WAN technology can also interconnect to a publicly shared network such as the Internet. This type of access must be obtained from an Internet Service provider (ISP). The IP protocol, which is a State standard, makes this connection seamless. This enhanced service creates an additional avenue for information and services, E-commerce and M-commerce, worldwide. Security and management procedures for the enterprise, become an additional concern with Internet access. Software tools must be in place along with policies that will manage and monitor the connection between the Internet and Enterprise network.

The Department of Information Technology (DOIT) provides WAN managed service for the executive branch of state government. In addition, DOIT acts as a hub for other branches of government providing, high speed interoperability, electronic access to services and exchange of information between state agencies. The telecommunications services supported by DOIT include data, and voice. Internet access is provided by DOIT for all branches of government (see Figure 3 below).

*Network Backbone Facilitie*s. Backbone facilities provide for the aggregation of an array of information, data, voice, video, and image services into a statewide transport mechanism. Compatibility with network access facilities is vital for connectivity. The planned future expansion of the network backbone facilities into regional metropolitan IP Optical Network hubs, will provide localization of traffic, improve performance, network flexibility and network content policy management. This technology will lower access costs per unit for transporting information. Migration to new technologies such as IP Optical Networks will pave the way towards advanced, cost-effective high-speed scalable connectivity.

*Network Access Facilitie*s. Access facilities provide a point of entry into the statewide network infrastructure. In today's environment, network access facilities are provided by a variety of technologies, including terrestrial fiber, hybrid coaxial wire, and wireless technologies. Access to the Department of Information Technology infrastructure should be transparent to the other connectivity components and compatible with industry established standards.

The state's strategy is to provide cost effective, ubiquitous service by leveraging its buying power. This strategy provides a variety of network access facilities, ensuring a range of services and efficient unit prices for clients.

1) Technology Components

The following technical components have been identified as necessary for the successful implementation of the statewide WAN.

Technology Component 1: Protocols

A communications protocol is a set of rules governing how computers exchange information with each other. Protocols were originally proprietary, for example IBM's SNA and Digital's DECnet. Today, the Internet uses protocols based on open standards. This permits connections between machines from many vendors.

Technology Component 2: Customer Premise Equipment (CPE)

Resources must be installed at the customer location to provide access from the local network to the WAN. This equipment includes:

A *Router is* a device that connects separate networks together. It forwards information packet and routes/bridges protocols via a WAN.

Channel Service Unit / Digital Service Unit (CSU/DSU) This is two units in one. The CSU is a digital interface device used to connect end-user equipment to the local digital telephone loop. The DSU is a device used in digital transmission for connecting data transmission equipment (DTE) such as a router, to data communication equipment (DCE) or a service.

Today, DOIT purchases these devices built into the router.

Technology Component 3: Carrier Services

These are comprised of various networking technologies offered by the telephone companies as a service. Services are typically broken into two categories: Switched (ATM, SMDS-DXI, Frame Relay, ISDN, DSL and wireless) and Non-Switched (DDS - Point-to-Point and Multi-point).

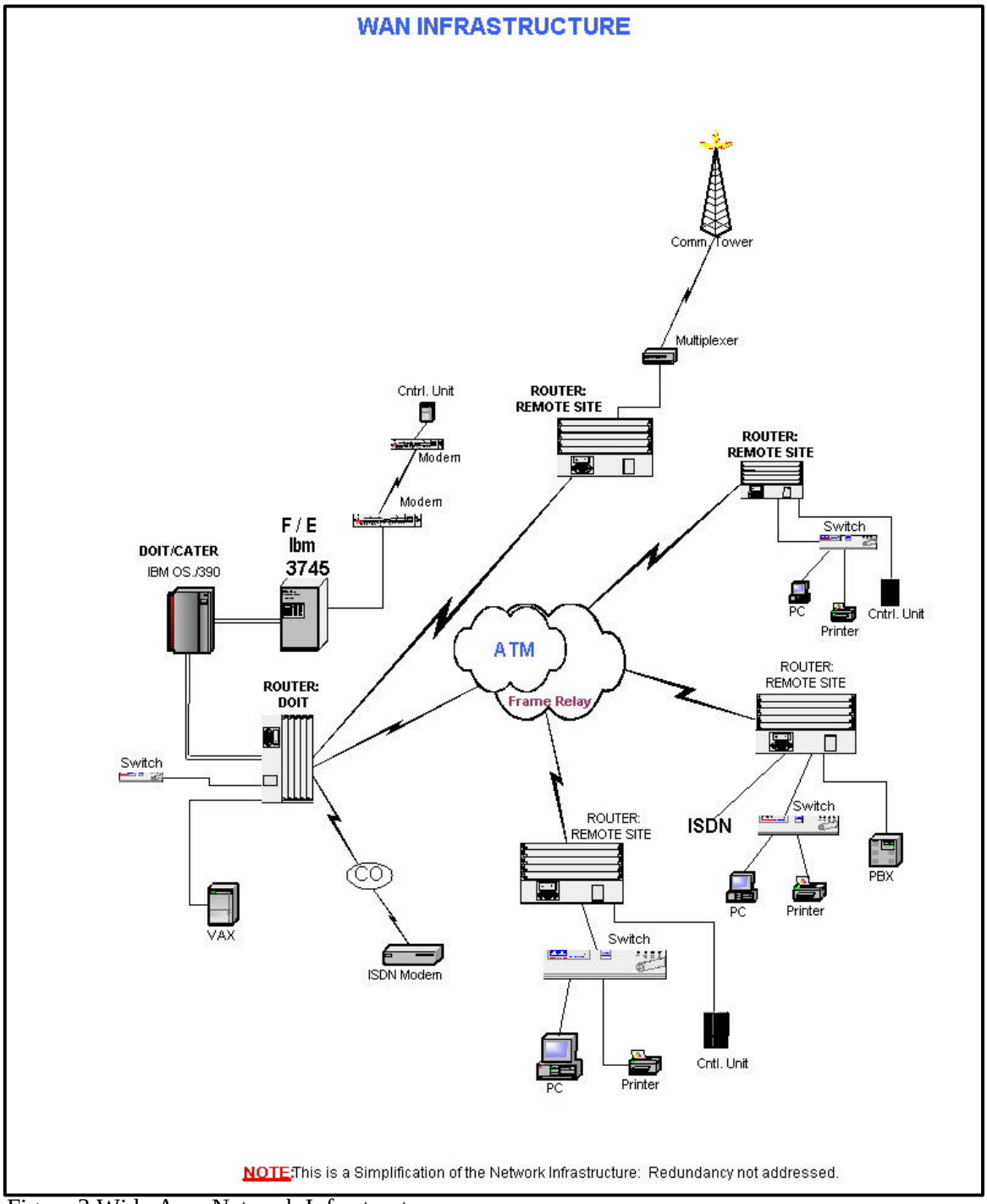

Figure 3 Wide Area Network Infrastructure

Technology Component 4: Internet Access

The Internet is a collection of networks with bridges or gateways between them. The protocol used by these networks is TCP/IP. Access to the Internet must be obtained from an Internet Service Provider (ISP). Connectivity to the ISP is mainly obtained in one of the following ways:

*Direc*t. The local network is connected to a WAN with Internet services. Any computer on the local network can then access sites on the Internet via the network. This access is permanently available.

Dial up access. A computer can use a modem (internal or external) to make a telephone call to an ISP or to access another computer that already has direct Internet access. The dial up connection can be generated using the Point to Point Protocol (PPP) or Serial Line Internet Protocol (SLIP). This allows the local computer to become a node on the Internet, with an IP address, for the period of connection. The machine dialed up will either assign a specific IP number each time (server allocation, PPP and SLIP) or give a number currently not in use (dynamic allocation in PPP). This access is only available for the length of the telephone call session.

2) Standards

In telecommunications, standards for products and services were created by the originating industry monopoly (i.e., the phone company). Therefore, although the monopoly has been disbanded, the proven standards that were established have remained. With data communications, however, there have always been many companies offering individual products and services. Therefore, although interim product standards have emerged as one company's product gained market share, there has been a lack of industry level standards. Therefore, until industry standards are established, an enterprise must choose to implement product based standards in order to create a manageable solution to the maintenance and management of its data communications infrastructure.

The following standards have been established for the implementation of agency-based components to connect with the statewide WAN. The goal is to employ open systems and industry approved standards, but a full complement of open standards does not yet exist for all components of WANs. Therefore, a combination of industry standards, de facto industry standards, and open standards are currently required to support a heterogeneous operating environment.

Standard 1: The WAN standard protocol is TCP/IP.

Rationale

- Open protocol.
- Allows Internet access.
- Allows for seamless integration of Intranet, Extranets and VPNs
- Supported by all vendors.

Standard 2: The standard internet access technology is Domain Name System (DNS) and IP address assignments are provided by Department of Information Technology (DOIT) for those agencies participating in the DOIT Enterprise Network Infrastructure.

Rationale

- DOIT must assign IP addresses to allow LANs access to the State WAN.
- All Internet access provided by the DOIT and is controlled by the state's Domain Name System.
- It allows a structured naming conviction and IP address allocation for the state's WAN and domain names.

- Non State entities, which want to connect to the State Infrastructure, must contact the DOIT networking DNS group before connecting.

Standard 3: When connecting to the State Infrastructure via the Internet, encryption must be used.

Rationale

- Federal and State guidelines and policies
- Access through the Internet to the State Intranet, VPN or SSL is required

Standard 4: Dialup remote access must use authentication and in some insistences encryption .

Rationale

- The State's ACE server authentication must be used when utilizing the State dialup network, (RNAS or Internet.
- Authentication/encryption is required accessing the State Intranet via Internet. This will be provided by DOIT.

3) Recommended Best Practices

These recommended best practices assist the state in the planning, design, implementation and expansion, administration, maintenance, and support of an interoperable statewide WAN architecture. The State has an existing policy on Network Security that addresses material relevant to Standards 3 and 4 above, and other architecture concerns as well. A copy of the policy is included in the appendix.

Best Practice 1: Develop an enterprise-wide network infrastructure that is scalable, centrally managed with quality of service (QOS), class of service (COS) and policy base.

Rationale

- A single uniform network infrastructure allows an enterprise to respond more efficiently when faced with requests by agencies for WAN component upgrades and installation.
- A centrally developed and managed infrastructure provides a more cost-effective use of infrastructure resources.
- Convergence of video, voice and data
- Agencies or business units should focus their WAN requirements on functional specifications such as level of service needed, throughput needed, and response time needed. The implementation of an appropriately responsive WAN should be a specialized function performed for the enterprise in its entirety.

Best Practice 2: When industry standards do not exist, use de-facto product standards

Rationale

- Use product based interim standards to simplify the process of developing and managing the enterprise WAN.
- There currently are no industry standards established for all the components of WAN design. Therefore, a product-based standard provides for consistency in the development, deployment, and management of WAN technology.

- The cooperative, collaborative, and geometric nature of WANs mandates that standards be used in order to build a cohesive WAN environment. Size alone prohibits a totally random, variable structure.

Transitional	Strategic Technology	Research / Evaluation
SNA, DECnet, X.25, proprietary protocols, etc.	TCP/IP	OSI
DDS point to point, Analog/DDS Multi-point	Frame Relay, ATM, Sonet, ISDN	IP Optical Networks, xDSL

Table 1-2. Implementation Approach for WANs

The implementation guidelines in this section pertain to WANs.

Best Practice 3: Configure WAN protocols using TCP/IP.

Rationale

- Open protocol.
- Allows Internet access.
- Allows creation of Intranets, extranets and VPNs
- Scaleable and flexible.

Best Practice 4: DOIT supports EIGRP on the routers in the infrastructure.

Rationale

- Εασε οφ Μαναγεμεντ
- Ρεδυνδανχψ

4) Guidelines

The implementation guidelines in this section pertain to WANs.

Guideline 1: Must contact Department of Information Technology (DOIT) for connection to the State Infrastructure.

Rationale

DOIT is responsible for designing, implementing and managing the State infrastructure.

C) WIRELESS : TDMA, CDMA, CDPD, GSM

There are multiple cellular carriers using multiple standards for wireless networking. Time Division Multiple Access, TDMA is one such standard. TDMA is a method of digital wireless communications transmission allowing a large number of users to access (in sequence) a single radio frequency channel without interference by allocating unique time slots to each user within each channel. TDMA technology is offered by AT&T for wireless service.

Code Division Multiple Access (CDMA) is a digital wireless technology developed by Qualcomm. CDMA is enabling new products and services from Palm-size Telephones to satellite

communications. CDMA networks are built with standard IP packet data protocols. Standard CDMAONE telephones already have TCP/IP and PPP protocols built into them.

Cellular Digital Packet Data (CDPD or Wireless IP) is a digital technology created specifically for sending data over the cellular network. It was developed by a consortium of leading wireless carriers, including Bell Atlantic Mobile, who designed its specification to be completely open. CDPD is based on TCP/IP, the data industry standard, so it's ready to work seamlessly with any Internet-based application. CDPD is also compatible with much of the hardware and software already on the market.

Global System for Mobile communications GSM is a digital communications technology developed in the early 1980s to allow for roaming throughout Europe. GSM is also a digital wireless technology. GSM is used mainly in Europe. Nokia supports this technology. TDMA and CDMA are used primarily in the United States.

1) Standards

There are multiple cellular carriers using multiple standards for wireless networking. Time Division Multiple Access, TDMA, Code Division Multiple Access (CDMA), Cellular Digital Packet Data (CDPD or Wireless IP) and Global System for Mobile communications (GSM). GSM is used mainly in Europe. Nokia supports this technology. TDMA and CDMA are used primarily in the United States.

Standard 1: TDMA, CDMA, CDPD and GSM for cellular telephone communications.

Rationale

- These standards are in common use by cellular carriers through which the state contracts services. Since universal geographic coverage by any single standard is not available, the use of multiple services using multiple standards is necessary.

2) Recommended Best Practices

These recommended best practices assist the state in the planning, design, implementation and expansion, administration, maintenance, and support of an interoperable statewide WAN architecture.

Best Practice 1: Still being developed

3) Guidelines

The implementation guidelines in this section pertain to Wireless

Guideline 1: Still being developed.

D) Video and Imaging

Technology advances during the last 10 years have provided a number of means to carry video signals over relatively low bandwidth (64k) network facilities. In addition, users have sometimes compromised their requirements where full motion video is not absolutely needed. Some of the earliest and least expensive systems utilizing data compression techniques and other digital video technologies offered low quality video services as compared to broadcast-quality services. These systems were relatively expensive ($50,000 and up per-end of a videoconferencing link) and they required fairly expensive and inflexible dedicated network facilities, such as T-1. As the market for systems utilizing compressed video transmission

techniques developed the capabilities increased and the costs declined. Eventually, systems were developed that utilized ISDN PRI and BRI facilities. The bandwidth for these systems could be adjusted to allow the user, on a connection-by-connection basis, to trade off between quality and bandwidth consumption. The PRI interfaced systems often utilize as little as 128kb/s of the facility, and can step up to 384kb/s, 768kb/s or full 1.544 Mb/s use of the PRI network service. This came about as part of ITU Px64 standards that served to allow bonded use of 64kb/s channels up to E-1 speeds of 2.048 Mb/s. Systems that offered BRI interface capabilities, although limited to low quality 128kb/s bandwidth, brought a high degree of flexibility through their ability to network to multiple locations on a switched basis.

1) Standards

Video and imaging systems have historically required very high bandwidth network facilities in order to carry the signal necessary to faithfully reproduce a transmitted signal at a receiving location. Traditional native video signal formats in use today (broadcast television and cable television channels) are analog in nature, and consume a bandwidth of approximately 6 MHz. This bandwidth could alternatively be used to carry 1200 or more, simultaneous standard telephone conversations. The information-intensive nature of video and imaging signals makes most voice and data bandwidth requirements seem small by comparison.

The combination of technology advances, market competition, and development of the Internet has enabled the development and use of video that utilizes very low bandwidth as it coexists with voice and data traffic on LANs and WANs. MPEG video standards were developed with the need for transmission over limited bandwidth as well as for random access for multimedia applications. Other standards and protocols have served to help facilitate the set up of video transmissions across LANs and WANs, and to improve the bandwidth control to enable these networks to provide consistent quality. These include ITU H.323 interoperability standards, IETF Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP).

Standard 1: H.320 interoperability standards.

Rationale

> This standard has been successfully deployed to enable videoconferencing systems to inter-operate using ISDN. The state's current systems comply with this standard, which was made a part of a statewide video conferencing contract.

Prospective Standards 2: ITU H.323 interoperability standards, IETF Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), Motion Pictures Experts Group standards (MPEG).

Rationale

> These standards will enable the state to provide transport for multimedia communications (voice, data, and video) as part of its strategy to merge voice and video services with data traffic for LAN and WAN transport over a packet-based (IP) infrastructure. MPEG standards will provide the state with a bandwidth/storage efficient means of utilizing video when stored and retrieved from servers.

2) Recommended Best Practices

These recommended best practices assist the state in the planning, design, implementation and expansion, administration, maintenance, and support of an interoperable statewide WAN architecture.

Best Practice 1: Still being developed

3) Guidelines

The implementation guidelines in this section pertain to Wireless

Guideline 1: Still being developed.

E) PBX

Technology Component: Private Branch Exchange (PBX)

A Private Branch Exchange, or PBX, performs the function of switching telephone calls among users connected to the PBX switching system. Users can be connected directly by cabling within a building or campus served by the PBX, or connected through wireless telephones, external cabled or wireless links to other PBX's in other geographic locations, and also via local exchange carrier trunks which provide the ability for the PBX to interconnect with any other party connected to the public switched telephone network.

1) Standards

A PBX performs the same basic function as do telephone carrier's switching systems, but for private, rather than public use. A number of users are connected to the system and can call other users on the same system, or they can call users external to the system through networked connections. These networked connections generally offer significantly less traffic capacity than the number of users could generate if all attempted to make calls external to the system simultaneously. The external traffic capacity should be set up to be sufficient, however, for the amount of traffic that is actually generated. An important aspect of the operation of the PBX is the monitoring of the traffic generated and the periodic adjustment to the network facilities to accommodate the anticipated traffic, but without over-sizing the network facilities. Additional functions of the PBX include:

- Voice mail systems, often integrated within the PBX, but sometimes an adjunct system.
- Generation of data for call accounting systems, which track calls made.
- Route selection, which determines the optimal network facilities to be used.
- Features such as conferencing, call distribution, and other user features.
- PBX manufacturers have developed network interface equipment and software to enable the PBX's to utilize IP networks. The voice traffic generated by the systems is transformed to a packet format in order to be integrated with data traffic on LANs and WANs.
  PBX systems utilize a variety of industry standards to accomplish this, and the PBX industry is historically strong in adhering to standards since the systems functionality is directly related to their ability to interconnect with other PBX's and with a variety of network facilities.

Standard 1: ISDN PRI compatibility.

Rationale

- Interoperability with network service providers.

Standard 2: Analog services compatibility.

Rationale

- Interoperability with network service providers.

Standard 3: T-1 compatibility.

Rationale

- Interoperability with network service providers.

2) Recommended Best Practices

These recommended best practices assist the state in the planning, design, implementation and expansion, administration, maintenance, and support of an interoperable statewide WAN architecture.

Best Practice 1: Still being developed

3) Guidelines

The implementation guidelines in this section pertain to Wireless

Guideline 1: Still being developed.

Product Selection

WAN : Cisco modular routers are the only products that meet all the principles based on input from the network domain team.

Switching

Pending an issuance of a RFP, and based on the as is analysis, two vendors, Cisco and Cabletron, currently dominate the switch install base. For multi-media applications that require managed bandwidth, Cisco is the recommended vendor of choice.

Telephony

- Still being researched
- SNET Eagle PBX - no longer being supported, replacement parts cannot be obtained for this model of PBX
- Cisco IP Phones – still in R+D
- Nitsuko PBX ‘s – product is no longer made, should be replaced ASAP.

Appendix – Network Security Policy and Procedures for use by all State Agencies

Version: 1.0 **Date Issued**: April 2, 1999 **Date Effective**: April 29, 1999

Purpose

The Department of Information Technology (DOIT) for the State of Connecticut, under the authority granted to the Chief Information Officer in Sec. 4d2. of the Connecticut General Statutes, has established this policy and reporting requirements, and associated standards to assure that critical information is protected and data flow is not interrupted by unauthorized access.

Policy Statements

The following policy statements are abstracted from the official State of Connecticut Network Security Policy.

1. All information travelling Over State computer networks that has not been specifically identified as the property of other parties will be treated as though it is a State asset. If there is no primary agency designated to administer this information, DOIT will become the steward of this data until another agency is designated. It is the policy of the State to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
2. In addition, it is the policy of the State to protect information belonging to third parties--that has been entrusted to the State in confidence--in the same manner as private sector trade secrets as well as in accordance with applicable contracts.
3. All computers permanently or intermittently connected to State of Connecticut networks, and all DOIT computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. must have password access controls. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.
4. The computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the need-to-know.
5. Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless the Agency System Administrator has identified, in writing, the security risk involved and submitted them to the Security Review Committee, and the Chief Information Officer has expressly accept these and other risks associated with the proposal.
6. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee.
7. Each agency that has existing dial-up lines/modems today must submit a request for consideration of approval to the Security Review Committee.
8. Wireless communications, or other broadcast technologies, must not be used for data transmission containing State "confidential" or "restricted" information unless the connection is encrypted and has an acceptable level user authentication.
9. Third party vendors must NOT be given dial-up privileges to State computers and/or networks unless the involved system administrator determines that they have a bone fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).
10. All users wishing to use the State internal networks, or multi-user systems that are connected

to the State internal networks, must sign a *compliance statement* prior to being issued a user-ID.

State workers in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing "restricted" or "confidential" State information must not leave these computers unattended at any time unless the information is stored in encrypted form. Transportable computers containing unencrypted "restricted" or "confidential" information must remain in the possession of the State worker traveler when traveling.

Implementation of the Policy

An Implementation Committee, composed of DOIT and other agency IT staff, will assist agencies in gaining initial compliance with this policy. The Implementation Committee will review the following actions by agencies:

Designate a information security liaison.

Each agency must determine what agency information is confidential or restricted, and submit this information in writing

Each agency that has existing dial-up lines/modems today must submit a request for review and approval.

An Agency that has it's own Internet connection today, must submit the following information:

1. Name of the Internet Provider and line speed of the circuit.
2. Model and type of Firewall hardware and software.
3. Port numbers that are opened in the Firewall.

The Security Review Committee will initially review:

1. Agency developed security policies.
2. Any modification in existing Network/Systems configurations that may not conform to the Statewide Security policy.

Agency Planning and Reporting Responsibilities

Planning:

4. Each State agency will develop it's own network security policy. The agency security policy will address:

a. System Access Control which includes how to choose passwords, how to set-up passwords and log-in/log-off procedures,
b. System Privileges; limiting system access, process for granting system privileges and the process for revoking system privileges and Establishment of Access Paths;
c. Computer Network Changes; conditions for participation in external networks, policy for initiating session via dial-up lines, establishing wireless communications and discussion of computer viruses, worms, and Trojan horses.

3. Each agency, must determine what agency information is confidential or restricted
4. The agency network security policy will be incorporated in the agency's Information Technology plan and architecture document.

Reporting:

5. As of July 1, 1999, each agency will submit the information required in **[**Attachment A**]** of

the official policy statement to to Jim McGill, Enterprise Network Manager.

6. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee

Any agency that has it's own Internet connection today or will have in the future, must submit the following information to the Security Review Committee:

a) Name of the Internet Provider and line speed of the circuit
b) Model and type of Firewall hardware and software.
c) c) Port numbers that are opened in the Firewall.

Compliance:

5. Each agency must submit it's own Network Security Policy to the Security Review Committee for review and approval.
7. Each State Agency must have a designated information security liaison. The name, telephone number and email address of the individual or individuals must be sent to Jim McGill. email address: james.mcgill@po.state.ct.us This information must come from the Commissioner or IT Manager level.

Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee.

Scope

This policy applies to the following entities: any State of Connecticut agency, institution, office, department, commission, council or instrumentality that utilizes State owned and maintained data networks in the conduct of its business.

Definitions

State Agency: For the purposes of this policy, the term *State Agency* refers to any State of Connecticut agency, institution, office, department, commission, council or instrumentality.

C*ompliant:* For the purposes of this policy, an agencies network security policy considered compliant when it meets the criteria defined in, and/or performs as described in, the State Network Security Policy.